

Sobre el Teorema de Burnside para Anillos de Matrices

On Burnside Theorem for Matrix Rings

Oswaldo Dede Mejía¹

¹Programa de Matemáticas
Universidad del Atlántico, Colombia
E-mail: dedemejia@gmail.com

María J. Ortega Wilches²

²Universidad Pedagógica Libertador, IPC Caracas, Venezuela
E-mail: mariajoseow@gmail.com

Alejandro Urieles Guerrero³

³Programa de Matemáticas
Universidad del Atlántico, Colombia
Dpto. Matemáticas Puras y Aplicadas
Universidad Simón Bolívar, Venezuela
E-mail: alejandrourieles@mail.uniatlantico.edu.co

Received / Recibido: 22/12/2013. Accepted / Aceptado: 6/02/2014

Resumen

Sea n un entero positivo y sea \mathbb{C} el campo de los complejos, denotemos por $M_n(\mathbb{C})$ el anillo de matrices $n \times n$ con entradas en \mathbb{C} . En el presente artículo se realiza un estudio del Teorema de Burnside en el contexto de los anillos de matrices $M_n(\mathbb{C})$, dando una demostración alternativa con herramientas básicas del álgebra.

Palabras claves: Campo de los números complejos, anillo de matrices $n \times n$ sobre el campo de los complejos, operadores lineales, matriz unitaria, subespacio propio.

Abstract

Let n be a integer non-negative and let \mathbb{C} be field of the complex, we denote $M_n(\mathbb{C})$ the matrix rings $n \times n$ with entries in \mathbb{C} . In the present paper we study the theorem of Burnside in the context of matrix rings $M_n(\mathbb{C})$, giving a alternative proof using basic concepts of the algebra.

Keywords: Field of the complex, the matrix rings $n \times n$ on \mathbb{C} , linear operators, unitary matrix, proper subspace.

1. Introducción

En 1.905 William Burnside publica el siguiente teorema conocido como Teorema de Burnside para grupos finitos de matrices invertibles $n \times n$: Si G es un grupo de matrices invertibles $n \times n$

con entradas en \mathbb{C} , entonces $\{0\}$ y \mathbb{C}^n son los únicos subespacios de \mathbb{C}^n invariantes por G si y sólo si G contiene n^2 matrices linealmente independientes. Este trabajo permitió que investigadores como Frobenius y Schur avanzaran en el estudio de la teoría de representación de grupos finitos,

demostrando ser un resultado fundamental para esta teoría (ver [6]).

En el presente trabajo se realiza un estudio del Teorema de Burnside en el contexto de los anillos de matrices tomando como base [3, 6, 7]. En la sección 2 damos algunas observaciones y resultados conocidos del álgebra que serán utilizados durante el trabajo.

Finalmente en la sección 3 estudiamos la demostración de una versión del Teorema de Burnside para anillos de matrices.

2. Preliminares

Las definiciones y resultados presentadas en esta sección pueden consultarse en [1, 2, 4]. Consideramos $M_n(\mathbb{C})$ el conjunto de matrices $n \times n$ con entradas en \mathbb{C} , es decir,

$$M_n(\mathbb{C}) = \left\{ \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} : a_{i,j} \in \mathbb{C}, 1 \leq i, j \leq n \right\} \quad (1)$$

Es sabido que (1) con las operaciones usuales tiene estructura de anillo.

OBSERVACIÓN 2.1. Para V y W espacios vectoriales sobre un campo K y $T : V \rightarrow W$ una transformación lineal se tiene:

- i) La imagen de T es $Im(T) = \{w \in W : T(v) = w, v \in V\}$,
- ii) El núcleo de T es el conjunto $\ker(T) = \{v \in V : T(v) = 0\}$,
- iii) El rango de T se define como la dimensión de su imagen. Así, $\text{rang}T = \dim(ImT)$,
- iv) La nulidad de T se define como la dimensión de su núcleo. Así, nulidad $T = \dim(Nu(T))$,
- v) Si V es de dimensión finita y $\{v_1, \dots, v_n\}$ es una base de V entonces cada $v \in V$ tiene

la forma $\sum_{i=1}^n c_i v_i$ para $c_i \in K$. Consecuentemente si $T \in L(V, W)$, se tiene

$$T(v) = \sum_{i=1}^n c_i T(v_i).$$

Por lo tanto, el conjunto $\{T(v_1), \dots, T(v_n)\}$ es un conjunto de generadores de ImT . Si este conjunto es linealmente independiente, entonces,

$$\text{rang}T = \dim(ImT) = n.$$

OBSERVACIÓN 2.2. Para V y W espacios vectoriales sobre un campo K y $L(V, W)$ el conjunto de todas las transformaciones lineales de V en W las siguientes afirmaciones se cumplen:

- i) $\dim V = \dim(Nu(T)) + \dim(ImT)$,
- ii) Si W es un subespacio de V entonces W es de dimensión finita y $\dim W \leq \dim V$,
- iii) Si W es un subespacio de V y $\dim V = n$ y $\dim W = n$, entonces $W = V$,
- iv) Si W es un espacio vectorial sobre un campo K , entonces $L(V, W)$ es también un espacio vectorial sobre K ,
- v) Si dimensión de V es n y si W es un espacio vectorial de dimensión finita m sobre K entonces el espacio $L(V, W)$ es de dimensión finita mn .

DEFINICIÓN 2.1. Sean V un K -espacio vectorial y T un operador lineal sobre V . Se dice que un subespacio W de V , es invariante por T si T aplica W en si mismo, esto es, si para todo $v \in W$, $T(v) \in W$.

DEFINICIÓN 2.2. Sean V un K -espacio vectorial y $T : V \rightarrow V$ un operador lineal. Un escalar $k \in K$ se llama un valor propio de T si existe un vector diferente de cero, $v \in V$, tal que $T(v) = kv$. Si k es un valor propio de T entonces cualquier vector $v \in V$ tal que $T(v) = kv$ se llama un vector propio de T asociado al valor propio k .

LEMA 1. Sea V un K -espacio vectorial y sean $T : V \rightarrow V$ un operador lineal y k un valor propio. El conjunto

$$E = \{v \in V : Tv = kv\}, \quad (2)$$

es un subespacio de V .

OBSERVACIÓN 2.3. El conjunto dado en (2) se denomina subespacio propio de T asociado al valor propio k .

LEMA 2. Sea $\{v_1, \dots, v_n\}$ una base de un espacio vectorial W sobre un campo K y sea w cualquier vector no cero de W . Existen escalares, a_i , $i = 1, \dots, n$, no todos cero, tales que

$$w = \sum_{i=1}^n a_i v_i, \quad a_i \in K.$$

Si a_k es diferente de cero, donde $k = \{1, \dots, n\}$, entonces $\{v_1, \dots, v_{k-1}, w, v_{k+1}, \dots, v_n\}$, es también una base de W .

DEFINICIÓN 2.3. Sea V un K -espacio vectorial con producto interno y dimensión finita. Una base β de V se dice base ortogonal si β es un conjunto ortogonal. Se dice que β es una base ortonormal si β es un conjunto ortonormal.

DEFINICIÓN 2.4. Una matriz cuadrada A sobre el campo de los números complejos se dice unitaria si $AA^* = I$ y $A^*A = I$ donde A^* es la adjunta de A . Es decir, $A^* = A^{-1}$.

OBSERVACIÓN 2.4. Una matriz cuadrada sobre un campo de los números complejos es unitaria si y sólo si sus columnas (filas) son vectores unitarios mutuamente ortogonales.

3. Teorema de Burnside para Anillos de Matrices Invertibles

En el contexto de la estructura de anillos de matrices, el Teorema de Burnside [3, 6] se enuncia así:

TEOREMA 1. Sea A un subanillo de $M_n(\mathbb{C})$ que contiene todas las matrices escalares. Si \mathbb{C}^n no contiene subespacios propios no triviales invariantes por A , entonces $A = M_n(\mathbb{C})$.

Para llegar a la demostración del teorema 1 se estudian los siguientes resultados.

LEMA 3. Sea $\mathcal{R} = M_n(\mathbb{C})$, el anillo de matrices $n \times n$ sobre \mathbb{C} y sea A un subanillo de \mathcal{R} que contiene todas las matrices escalares tal que \mathbb{C}^n no contiene subespacios no triviales invariantes por A . Si $g \in \mathcal{R}$, y para todo $f \in A$, $gf = fg$, entonces g es una matriz escalar, es decir $g = kI$ para algún $k \in \mathbb{C}$.

Demostración. Sea $g \in \mathcal{R}$, tal que g conmuta con todo elemento de \mathcal{R} . Sea $k \in \mathbb{C}$ un valor propio de g , el subespacio propio asociado a k es

$$E_k = \{v \in \mathbb{C}^n : g(v) = kv\} \subseteq \mathbb{C}^n,$$

sea además $f \in A$. Como por hipótesis $gf = fg$, entonces, $g(fv) = f(gv) = f(kv) = kfv$, para $v \in E$, esto es,

$$gfv = kfv,$$

se observa que $fv \in E_k$ y $fE_k \subseteq E_k$, es decir, E_k es invariante por f .

Ahora bien, como $E_k \neq \{0\}$ y por hipótesis, \mathbb{C}^n no contiene subespacios no triviales invariantes por A , entonces, $E_k = \mathbb{C}^n$. Esto significa que para todo $v \in \mathbb{C}^n$, $gv = kv = kv$, esto es, $g = kI$, es decir, g es una matriz escalar como se quería demostrar. \square

LEMA 4. Sea $\mathcal{R} = M_n(\mathbb{C})$ el anillo de matrices $n \times n$ sobre \mathbb{C} y sea A un subanillo de \mathcal{R} que contiene todas las matrices escalares, tal que \mathbb{C}^n no contiene subespacios no triviales invariantes por A . Si $v \in \mathbb{C}^n$ y W es un subespacio de \mathbb{C}^n tales que para cualquier $f \in A$, $f(W) = 0$ implica $fv = 0$, entonces $v \in W$.

Demostración. Se procede por inducción sobre $\dim W$, la dimensión de W .

Si $\dim W = 0$; $0 = W$. Como por hipótesis, A es un subanillo de $M_n(\mathbb{C})$ que contiene las matrices escalares, entonces A contiene I_n , elemento identidad para la multiplicación, el cual satisface

$$I_n W = I_n 0 = 0,$$

en consecuencia, si $v \in \mathbb{C}^n$ es tal que para todo $f \in \mathcal{R}$, $fW = 0$ implica $fv = 0$, en particular, $I_n v = 0$, esto es $v = 0$. Así $v \in W$.

Se considera ahora el caso en que $\dim W = k > 1$.

Sea W_0 un subespacio propio de W , tal que $\dim W_0 = \dim W - 1$. Una base $\{v_1, \dots, v_{k-1}\}$ de W_0 se puede extender a una base $\{v_1, \dots, v_{k-1}, w\}$ para algún $w \in W$, entonces, si $u \in W$, existen escalares c_1, \dots, c_{k-1}, c tales que

$$u = (c_1 v_1 + \dots + c_{k-1} v_{k-1}) + cw,$$

pero $w_0 = c_1 v_1 + \dots + c_{k-1} v_{k-1} \in W$, esto es $u = w_0 + cw$, donde $w_0 \in W_0$ y $cw \in C_w = \{aw : a \in \mathbb{C}\}$, entonces $W = W_0 + C_w$.

Sea

$$H = \{h \in A : hW_0 = 0\} \subseteq A,$$

H es un subespacio de A , para verlo, sean $h_1, h_2 \in H$, y, $w_0 \in W_0$. Entonces se tiene

$$(h_1 + h_2)(w_0) = h_1(w_0) + h_2(w_0) = 0 + 0 = 0.$$

Así, $h_1 + h_2 \in H$. Además, si $c \in \mathbb{C}$ y $h \in A$,

$$(ch)(w_0) = c(h(w_0)) = c0 = 0,$$

es decir, $ch \in H$.

Al aplicar la hipótesis inductiva a W_0 , se tiene que, si para todo $f \in A$, $f(W_0) = 0$ implica que $f(v) = 0$, entonces $v \in W_0 = 0$.

Como $w \notin W$, para algún $f \in A$, $f(w) \neq 0$ entonces, $Hw = \{hw : h \in H\} \neq 0$.

Además, si $f \in A$, $h \in H$ y $w_0 \in W_0$ entonces

$$(fh)(w_0) = f(h(w_0)) = f(0) = 0.$$

Esto es, $fh \in H$ con lo que $AH \subseteq H$, en consecuencia

$$A(H(w)) \subseteq H(w),$$

esto significa que $H(w)$ es un subespacio no trivial invariante por A , lo cual implica que $H(w) = \mathbb{C}^n$.

Se considera ahora la transformación lineal

$$g : \mathbb{C}^n \longrightarrow \mathbb{C}^n,$$

tal que,

$$g(h(w)) = h(v), \forall h \in H.$$

g está bien definida, ya que, si $h_1, h_2 \in H$ y $h_1(w) = h_2(w)$, entonces

$$(h_1 - h_2)v = 0.$$

Así, $h_1 v - h_2 v = 0$, entonces, $h_1 v = h_2 v$, por lo tanto $g(h_1 w) = g(h_2 w)$.

Se verifica ahora que g es lineal, ya que,

$$\begin{aligned} g(h_1 w + h_2 w) &= g((h_1 + h_2)w) = (h_1 + h_2)v \\ &= h_1 v + h_2 v = g(h_1 w) + g(h_2 w). \end{aligned}$$

También,

$$g(ch_1 w) = (ch_1)v = ch_1(v) = cg(h_1 w).$$

Ahora se prueba que g conmuta con cualquier $f \in A$, en efecto,

$$\begin{aligned} gf(h(w)) &= g((fh)(w)) = (fh)(v) \\ &= f(h(v)) = f(gh(w)) \\ &= (fg)(h(w)) \forall h \in H. \end{aligned}$$

De acuerdo al lema, 3

$g = kI$ para algún $k \in \mathbb{C}$, con lo que

$$\begin{aligned} h(v) &= g(h(w)) = kI(h(w)) \\ &= k(Ih(w)) = k(Ih)w = kh(w). \end{aligned}$$

En consecuencia,

$$h(v) - kh(w) = h(v - kw) = 0, \forall h \in H.$$

De donde, $v - kw \in W_0$, así, $v - kw = w_0 \in W_0$.

Entonces,

$$v = w_0 + kw, k \in \mathbb{C}$$

$$v = w_0 + w_1,$$

donde $w_0 \in W_0$ y $w_1 \in C_w$, es decir, $v \in W$, como se deseaba demostrar. \square

Ahora, podemos demostrar el teorema 1 usando los resultados anteriores.

4. Demostración del Teorema 1

Si se prueba que A contiene a $\{E_{i,j} : i, j = 1, \dots, n\}$, la base canónica de $M_n(\mathbb{C})$, se tiene que $M_n(\mathbb{C}) \subseteq A$ y por tanto $M_n(\mathbb{C}) = A$. Así, para probar el teorema 1 basta probar que A contiene todas las matrices $E_{i,j}$.

Sea $\beta = \{e_1, \dots, e_n\}$, la base canónica de \mathbb{C}^n . β es una base ortonormal. Sea W_0 el subespacio generado por $\{e_2, e_3, \dots, e_n\}$ y sea

$$H = \{h \in A : hW_0 = 0\}.$$

H es subespacio de A .

Puesto que $e_1 \notin W$ entonces existe $h \in H$ tal que $h(e_1) \neq 0$ y, dado que $H(e_1)$ es invariante por A

entonces $H(e_1) = \mathbb{C}^n$. En particular, para cada i existe $h_i \in H$ tal que $h_i(e_{j,i}) = 0$, para $j \neq i$.

La matriz de h_i es $E_{i,1}$. Por lo tanto, $E_{i,j} \in A$ como se deseaba demostrar. \square

Referencias

- [1] M.A. Armstrong, Groups and Symmetry. Springer - Verlag, 1988.
- [2] J. Dorronsoro, E. Hernández, Números, Grupos y Anillos, Editorial Addison-Wesley, 1996.
- [3] I. Halperin and P. Rosenthal, Burnside theorem on Algebras of Matrices. Amer. Math. Monthly 87 (1980) 810.
- [4] K. Hofman y R. Kunze, Álgebra Lineal. Prentice Hall, 1973.
- [5] T. Hungerford, Álgebra. Springer - Verlag, 1974.
- [6] T.Y. Lam, A theorem of Burnside on Matrix Rings. AmerMath. Math. Monthly 105(1998).651-653.
- [7] V. Lomonosov, P. Rosenthal, The Simplest Proof of Burnside Theorem on Matrix Álgebras, Linear Álgebra and Its Applications 386 (2004) 45-47.

Para citar este artículo: Urieles A et al. 2014, "Sobre el Teorema de Burnside para Anillos de Matrices". Disponible en Revistas y Publicaciones de la Universidad del Atlántico en: <http://investigaciones.uniatlantico.edu.co/revistas/index.php/MATUA>.